What is claimed is:

Claim 1. A remote security key encoding system comprising:

a client system containing a client identity, a client location and client account information;

a service provider system connected to the client system via an Internet connection;

a financial institution system, connected to the client system and the service provider system via the Internet, such that, when, over the Internet a client requests the encoding of a security key, the service provider system identifies the client, authenticates the client location, confirms that the client's account status is above some predetermined threshold, and encodes the security key per the client request.

Claim 2. The encoding system as in claim 1, wherein the client system comprises an electronic lock, a lock-key interface, an on-site encoder, and a client computer system, the client computer system being capable of accessing the Internet.

Claim 3. The encoding system as in claim 2, wherein the client computer system accesses the Internet via an Internet service provider.

Claim 4. The encoding system as in claim 2, wherein the service provider system comprises a service provider account, billing software, electronic funds transfer software, authorization software, a customer database having client identification data, and a client service module.

Claim 5. The encoding system as in claim 4, wherein the service provider system is remotely located in a remote server.

Claim 6. The encoding system as in claim 5, wherein the financial institution system comprises software for providing electronic verification of a client's account status and software for electronically transferring funds from the client's account to the service provider's account.

Claim 7. The encoding system as in claim 6, wherein the remote server contains software for encoding security keys.

Claim 8. The encoding system as in claim 7, wherein the remote server contains software for authorizing security key system functions upon a request by the client.

Claim 9. A method for remotely authorizing a request to encode security keys from a service provider by a client, comprising the following steps:

matching the query to a specific client account, the client account having a unique client number with client information stored remotely in a client database;

verifying that the client request came from an authorized property properly requesting keys be made; and

verifying that the client is current on all billing and that the client account has a positive balance therein.

Claim 10. The method for remotely authorizing a client request as in claim 9, wherein the step of verifying that the client is current on all billing, further comprises the steps of:

confirming that the client number and client information match the data stored in the client database, and if the data matches; then

granting access to the account data by the client.

Claim 11. The method for remotely authorizing a client request as in claim 10, wherein the step of verifying that the client is current on all billing, further comprises the steps of:

comparing the account balance with a critical account amount, the critical account amount being selected by the service provider and the client, and if the account balance is greater than the critical account amount; then

communicating to the client that the request has been authorized; and

issuing the client an encrypted key code.

Claim 12. The method for remotely authorizing a client request as in claim 11, wherein the step of verifying that the client is current on all billing, further comprises the steps of:

comparing the account balance with a minimum account amount determined by the service provider and the client, the minimum account amount being an amount in the account below which all additional requests are denied; and if the account balance is greater than the minimum account amount but less than the critical account amount; then

communicating to the client that the request has been authorized; and

attaching a warning notice to the client along with the authorization, informing the client that the account balance is below the critical amount.

Claim 13. The method for remotely authorizing a client request as in claim 12, wherein the step of verifying that the client is current on all billing, wherein if the account balance is less than the minimum account amount, the following steps are taken:

denying the transaction;

electronically communicating with the client that the transaction is denied because the minimum account balance was reached.

Claim 14. A method for remotely authorizing a request to encode security keys from a service provider by a client, comprising the following steps:

matching the query to a specific client account, the client account having a unique client number with client information stored remotely in a client database,

verifying that the client request came from an authorized property properly requesting keys be made and, if so,

accessing the client data for the client,

determining whether the date of the request is before or after a predetermined client payment date,

if before the client payment date, authorizing the client request, and

if after the client payment date, determining whether an electronic funds transfer was made from the client into the client account, and if the electronic funds transfer was successful, authorizing the request.

Claim 15. The method for remotely authorizing a request to encode security keys from a service provider by a client as in claim 14, further comprising the steps of:

raising a flag whenever an electronic funds transfer request made by the service provide to the client is unsuccessful,

if the flag has been raised, confirming whether a balance reflected in the client account is greater than zero, and

if the client account balance is greater than zero, authorizing the request, and

communicating a warning message to the client that the electronic funds transfer was unsuccessful and giving the state of the account.

Claim 16. The method for remotely authorizing a request to encode security keys from a service provider by a client as in claim 15, wherein if the flag is raised, and the account balance is zero or below, then further comprising the steps of:

denying the request, and

communicating a warning message to the client that the electronic funds transfer was unsuccessful and giving the state of the account.

Claim 17. The method for remotely authorizing a request to encode security keys from a service provider by a client as in claim 16, wherein the balance in the client account is some unit of exchange, comprising individual room nights or a number of security keys.

Claim 18. A method for billing a client that makes a request for remotely encoded security keys, comprising the steps of:

periodically querying each customer account,

noting an account balance,

comparing the account balance in each customer's account to a predetermined replenish amount,

if the customer account is greater than the replenish amount, completing the billing program with an indication that the request be approved;

if the customer account is less than the replenish amount, sending a request to a financial institution identified by the client for funds to be transferred electronically into the client's account, and

verifying that the electronic funds transfer was successful;

if the electronic funds transfer is successful, then updating the customer account information to reflect the electronic funds transfer, and

completing the billing program with an indication that the request be approved,

if the electronic funds transfer is unsuccessful, then communicating electronically the failed funds transfer request.

Claim 19. A method for billing a client that makes a request for remotely encoded security keys, comprising the steps of:

matching the query to a specific client account, the client account having a unique client number with client information stored remotely in a client database,

verifying that the client request came from an authorized property properly requesting keys be made and, if so,

accessing the client account to determine an actual usage fee equal for services rendered to date,

determining the date of the request,

if the request is on the first day of the month, comparing the actual usage fee with a predetermined minimum monthly fee,

if the actual usage fee is less than the minimum monthly fee, invoicing the client requesting that funds sufficient to restore the account to the minimum monthly balance are transferred electronically into the client's account,

verifying that the electronic funds transfer is successful;

if the electronic funds transfer is successful, then clearing an electronic funds transfer flag and setting an electronic funds transfer counter to zero;

if the electronic funds transfer is not successful, then setting the electronic funds transfer flag and increasing the electronic funds transfer counter by a specified increment;

comparing the electronic funds transfer counter to a predetermined number equal to the maximum allowable electronic funds transfer attempts, and

if the electronic funds transfer counter is less than this predetermined number, then authorizing the client's request,

communicating a warning message to the informing the client of the electronic funds transfer attempts and the client account status.

Claim 20. The method for billing a client that makes a request for remotely encoded security keys, as in claim 19, wherein the request is denied if the electronic funds transfer counter is greater than this predetermined number, and a message communicating the reasons for the transaction denial is submitted to the client.

Claim 21. The method for billing a client that makes a request for remotely encoded security keys, as in claim 19, where the request is made on a date other than the first day of the month, further comprising the steps of:

comparing the actual usage fee with a predetermined minimum monthly fee,

if the actual usage fee is less than the minimum monthly fee, authorizing the request,

if the actual usage fee is greater than the minimum monthly fee, determining whether the electronic funds transfer flag is set,

if the electronic funds transfer flag is set, meaning that one or more unsuccessful electronic funds transfer attempts have occurred, comparing the electronic funds transfer counter to a predetermined number equal to the maximum allowable electronic funds transfer attempts, and

if the electronic funds transfer counter is less than this predetermined number, then authorizing the client's request, and communicating a warning message informing the client of the electronic funds transfer attempts,

if the electronic funds transfer counter is greater than this predetermined number, then denying the client's request,

if the electronic funds transfer flag is not, the request is approved.

Claim 22. A method for a client to replenish a client account, in which the client has direct access to the client account, comprising the steps of:

accessing the client account by the client,

determining how much credit the client would like to place on the account,

specifying from which financial institution the funds should originate

generating an electronic funds transfer of the funds from the financial institution into the client's account,

determining whether the electronic funds transfer is successful, and if so,

updating the client account,

if the electronic funds transfer is unsuccessful, communicating this fact to the client.

Claim 23. The method for a client to replenish a client account as in claim 22, where the client accesses the client account via the Internet.